



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
**«МИРЭА – Российский технологический университет» РТУ
МИРЭА**

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Прикладные информационные технологии»

Практическая работа № 7
по дисциплине «Безопасность Операционных систем»
«Безопасность в Linux»

Москва 2021

Задание на практику:

Управление локальными пользователями и группами Linux

1. Создайте пользователя user, сделав его участником группы wheel

2. Убедитесь, что пользователь был создан и задайте пароль для него

- `$ tail -2 /etc/passwd`

- `$ passwd user`

3. Войдите в учетную запись user и изучите сведения о пользователе, группе и отобразите текущий каталог.

4. Просмотрите переменные, которые указывают на домашний каталог и пути, где происходит поиск исполняемых файлов

5. Войдите в учетную запись root, используя команду su

6. Повторите действия 3, 4

7. Войдите в учетную запись root, используя команду su -

8. Повторите действия 3, 4

9. Проанализируйте разницу

10. Изучите последние строки в /var/log/messages

11. Выполните команды от пользователя user

- `$ echo "nameserver 1.1.1.1" | tee -a /etc/resolv.conf /dev/null`

- `$ echo "nameserver 1.1.1.1" | sudo tee -a /etc/resolv.conf /dev/null`

- \$ vi /etc/motd
- \$ sudo vi /etc/motd

12. Проанализируйте разницу

Разрешения файловой системы

permissions	user	group	size	date	file/directory
drwxr-xr-x	2 paul	users	1024	Jan 2 23:50	.
drwxr-xr-x	6 root	root	1024	Jan 2 22:51	..
drwxr-xr-x	3 paul	users	1024	Jan 8 11:42	grassdata
lrwxrwxrwx	1 paul	users	13	May 6 1998	latex -> /d2/lt
drwx-----	2 paul	users	1024	Mar 8 17:30	mail
drwx-----	2 paul	users	1024	Feb 4 01:09	projects
-rw-r--r--	1 paul	users	844344	Dec 9 1998	nations.ps
-rw-rw-r--	1 paul	users	21438	Mar 2 21:47	ps4mf.txt

other (world) permissions

group permissions

user permissions

d : directory

- : file

l : link (to other file/directory)

r : read permission

w : write permission

x : execute permission (programm)

- : permission not set

Linux File Permission Codes

Permissions	Binary	Octal	Description
---	000	0	No permissions
--x	001	1	Execute-only permission
-w-	010	2	Write-only permission
-wx	011	3	Write and execute permissions
r--	100	4	Read-only permission
r-x	101	5	Read and execute permissions
rw-	110	6	Read and write permissions
rwX	111	7	Read, write, and execute permissions

Разрешения по умолчанию

umask Value Octal (xyz)	Default File Permissions	666 - xyz	Default Directory Permissions	777 - xyz
000	rw-rw-rw	666	rw-rw-rw	777
002	rw-rw-r--	664	rw-rw-r-x	775
022	rw-r--r--	644	rw-r--r-x	755
026	rw-r-----	640	rw-r--x--	751
046	rw--w----	620	rw-r--x--	731
062	rw----r--	604	rw-r--x--	715
066	rw-----	600	rw-r--x--	711
222	r--r--r--	444	r-xr-xr-x	555
600	---rw-rw-	066	--xrw-rw	177
666	-----	000	--x--x--	111
777	-----	000	-----	000

13. Отобразите значение по умолчанию для пользователя user

- \$ umask

14. Создайте директорию и файл, чтобы увидеть как пользовательская маска влияет на разрешения.

- \$ mkdir /tmp/catalog
- \$ ls -ld /tmp/catalog
- \$ touch /tmp/catalog/file
- \$ ls -l /tmp/catalog/file

15. Измените маску user таким образом, чтобы новые файлы создавались с доступом только на чтение для группы и без прав доступа для других пользователей.

- \$ umask 027
- \$ touch /tmp/catalog/file_1
- \$ ls -l /tmp/catalog/file_1

16. Измените маску по умолчанию для пользователя user, чтобы запретить весь доступ для пользователей, не относящихся к группе.

- `$ echo "umask 007" » ~/.bashrc`
- `$ cat ~/.bashrc`

17. Войдите еще раз от имени пользователя user, и проверьте сохранилась ли измененная маска.

- `$ umask`

ACL

18. Создайте файл /directory/file и группу workers. Добавьте пользователя user в группу workers. Измените группу владельцев directory на workers.

- `# groupadd workers`
- `# usermod -G workers user`
- `# mkdir /directory`
- `# echo "Hello from file" > /directory/file`
- `# chown -R :workers /directory`

19. Войдите в систему под пользователем user.

Например:

```
$ su - user
```

Прочтите файл:

```
$ cat /directory/file
```

20. Установите ACL для пользователя user, таким образом, чтобы он не имел доступа ни к существующим файлам, ни к созданным в будущем в каталоге /directory.

```
# setfacl -Rm u:user:- /directory
```

```
# setfacl -m d:u:user:- /directory
```

21. Попробуйте прочесть файл /directory/file и создать новый

22. Просмотрите и проанализируйте ACL для /directory

```
# getfacl /directroy
```